Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*

Adopted on 23 July 2020

This document aims at presenting answers to some frequently asked questions received by supervisory authorities ("SAs") and will be developed and complemented along with further analysis, as the EDPB continues to examine and assess the judgment of the Court of Justice of the European Union (the "Court").

The judgment C-311/18 can be found here, and the press release of the Court may be found here.

1) What did the Court rule in its judgment?

➔ In its judgment, the Court examined the validity of the European Commission's Decision 2010/87/EC on Standard Contractual Clauses ("SCCs") and considered it is valid. Indeed, the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred.

However, that validity, the Court added, depends on whether the 2010/87/EC Decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.

In that regard, the Court points out, in particular, that the 2010/87/EC Decision imposes an obligation on a data exporter and the recipient of the data (the "data importer") to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether that level of protection is respected in the third country concerned, and that the 2010/87/EC Decision requires the data importer to inform the data exporter of any inability to comply with the standard data protection clauses, and where necessary with any supplementary measures to those offered by those clause, the data exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the data importer

➔ The Court also examined the validity of the Privacy Shield Decision (Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield), as the transfers at stake in the context of the national dispute leading to the request for preliminary ruling took place between the EU and the United States ("U.S.").

The Court considered that the requirements of U.S. domestic law, and in particular certain programmes enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes, result in limitations on the protection of personal data which are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law[1], and that this legislation does not grant data subjects actionable rights before the courts against the U.S. authorities.

As a consequence of such a degree of interference with the fundamental rights of persons whose data are transferred to that third country, the Court declared the Privacy Shield adequacy Decision invalid.

2) Does the Court's judgment have implications on transfer tools other than the Privacy Shield?

➔ In general, for third countries, the threshold set by the Court also applies to all appropriate safeguards under Article 46 GDPR used to transfer data from the EEA to any third country. U.S. law referred to by the Court (i.e., Section 702 FISA and EO 12333) applies to any transfer to the U.S. via electronic means that falls under the scope of this legislation, regardless of the transfer tool used for the transfer[2].

3) Is there any grace period during which I can keep on transferring data to the U.S. without assessing my legal basis for the transfer?

➔ No, the Court has invalidated the Privacy Shield Decision without maintaining its effects, because the U.S. law assessed by the Court does not provide an essentially equivalent level of protection to the EU. This assessment has to be taken into account for any transfer to the U.S.

4) I was transferring data to a U.S. data importer adherent to the Privacy Shield, what should I do now?

➔ Transfers on the basis of this legal framework are illegal. Should you wish to keep on transferring data to the U.S., you would need to check whether you can do so under the conditions laid down below.

5) I am using SCCs with a data importer in the U.S., what should I do?

➔ The Court found that U.S. law (i.e., Section 702 FISA and EO 12333) does not ensure an essentially equivalent level of protection.

[1] The Court underlines that certain surveillance programmes enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes do not provide for any limitations on the power conferred on the U.S. authorities, or the existence of guarantees for potentially targeted non-US persons.

[2] Section 702 FISA applies to all "electronic communication service provider" (see the definition under 50 USC § 1881(b)(4)), while EO 12 333 organises electronic surveillance, which is defined as the "acquisition of a non-public communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter" (3.4; b)).

Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.

If you come to the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, you are required to suspend or end the transfer of personal data. However, if you are intending to keep transferring data despite this conclusion, you must notify your competent SA[3].

6) I am using Binding Corporate Rules ("BCRs") with an entity in the U.S., what should I do?

➔ Given the judgment of the Court, which invalidated the Privacy Shield because of the degree of interference created by the law of the U.S. with the fundamental rights of persons whose data are transferred to that third country, and the fact that the Privacy Shield was also designed to bring guarantees to data transferred with other tools such as BCRs, the Court's assessment applies as well in the context of BCRs, since U.S. law will also have primacy over this tool.

Whether or not you can transfer personal data on the basis of BCRs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. These supplementary measures along with BCRs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.

If you come to the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, you are required to suspend or end the transfer of personal data. However if you are intending to keep transferring data despite this conclusion, you must notify your competent SA[4].

7) What about other transfer tools under Article 46 GDPR?

➔ The EDPB will assess the consequences of the judgment on transfer tools other than SCCs and BCRs. The judgement clarifies that the standard for appropriate safeguards in Article 46 GDPR is that of "essential equivalence".

As underlined by the Court, it should be noted that that Article 46 appears in Chapter V GDPR, and, accordingly, must be read in the light of Article 44 GDPR, which lays down that "*all provisions in that chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by that regulation is not undermined*".

[3] See in particular recital 145 of the Court's judgment, and Clause 4(g) Commission decision 2010/87/EU, as well as Clause 5(a) Commission Decision 2001/497/EC and Annex Set II (c) of Commission Decision 2004/915/EC.

[4] See in particular recital 145 of the Court's judgment and Clause 4(g) of Commission Decision 2010/87/EU. See also Section 6.3 WP256 rev.01 (Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in BCRs, endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109), and Section 6.3 WP257 rev.01 (Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor BCRs, endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

8) Can I rely on one of the derogations of Article 49 GDPR to transfer data to the U.S.?

➔ It is still possible to transfer data from the EEA to the U.S. on the basis of derogations foreseen in Article 49 GDPR provided the conditions set forth in this Article apply. The EDPB refers to its guidelines on this provision[5].

In particular, it should be recalled that when transfers are based on the consent of the data subject, it should be:

- explicit,
- specific for the particular data transfer or set of transfers (meaning that the data exporter must make sure to obtain specific consent before the transfer is put in place even if this occurs after the collection of the data has been made), and
- informed, particularly as to the possible risks of the transfer (meaning the data subject should also informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented).

With regard to transfers necessary for the performance of a contract between the data subject and the controller, it should be borne in mind that personal data may only be transferred when the transfer is occasional. It would have to be established on a case-by-case basis whether data transfers would be determined as "occasional" or "non-occasional". In any case, this derogation can only be relied upon when the transfer is objectively necessary for the performance of the contract.

In relation to transfers necessary for important reasons of public interest (which must be recognized in EU or Member States'[6] law), the EDPB recalls that the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organisation, and that although this derogation is not limited to data transfers that are "occasional", this does not mean that data transfers on the basis of the important public interest derogation can take place on a large scale and in a systematic manner. Rather, the general principle needs to be respected according to which the derogations as set out in Article 49 GDPR should not become "the rule" in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.

9) Can I continue to use SCCs or BCRs to transfer data to another third country than the U.S.?

➔ The Court has indicated that SCCs as a rule can still be used to transfer data to a third country, however the threshold set by the Court for transfers to the U.S. applies for any third country. The same goes for BCRs.

The Court highlighted that it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice. If this is not the case, you should assess whether you can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA, and if the law of the third country will not impinge on these supplementary measures so as to prevent their effectiveness.

[5] See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, p.3.
[6] References to "Member States" should be understood as references to "EEA Member States".

You can contact your data importer to verify the legislation of its country and collaborate for its assessment. Should you or the data importer in the third country determine that the data transferred pursuant to the SCCs or to the BCRs are not afforded a level of protection essentially equivalent to that guaranteed within the EEA, you should immediately suspend the transfers. In case you do not, you must notify your competent SA[7].

➔ Although, as underlined by the Court, it is the primary responsibility of data exporters and data importers to assess themselves that the legislation of the third country of destination enables the data importer to comply with the standard data protection clauses or the BCRs, before transferring personal data to that third country, the SAs will also have a key role to play when enforcing the GDPR and when issuing further decisions on transfers to third countries.

As invited by the Court, in order to avoid divergent decisions, they will thus further work within the EDPB in order to ensure consistency, in particular if transfers to third countries must be prohibited.

10) What kind of supplementary measures can I introduce if I am using SCCs or BCRs to transfer data to third countries?

➔ The supplementary measures you could envisage where necessary would have to be provided on a case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to check if it ensures an adequate level of protection.

The Court highlighted that it is the primary responsibility of the data exporter and the data importer to make this assessment, and to provide necessary supplementary measures.

The EDPB is currently analysing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, whether legal, technical or organisational measures, to transfer data to third countries where SCCs or BCRs will not provide the sufficient level of guarantees on their own.

➔ The EDPB is looking further into what these supplementary measures could consist of and will provide more guidance.

11) I am using a processor that processes data for which I am responsible as controller, how can I know if this processor transfers data to the U.S. or to another third country?

➔ The contract you have concluded with your processor in accordance with Article 28.3 GDPR must provide whether transfers are authorised or not (it should be borne in mind that even providing access to data from a third country, for instance for administration purposes, also amounts to a transfer).

➔ Authorization has also to be provided concerning processors to entrust sub-processors to transfer data to third countries. You should pay attention and be careful, because a large variety of computing solutions may imply the transfer of personal data to a third country (e.g., for storage or maintenance purposes).

[7] See in particular recital 145 of Court's judgment . In relation to SCCs, see Clause 4(g) Commission Decision 2010/87/EU, as well as Clause 5(a) Commission Decision 2001/497/EC and Annex Set II (c) Commission Decision 2004/915/EC. In relation to BCRs, see Section 6.3 WP256 rev.01 (endorsed by the EDPB), and Section 6.3 WP257 rev.01 (endorsed by the EDPB).

12) What can I do to keep using the services of my processor if the contract signed in accordance with Article 28.3 GDPR indicates that data may be transferred to the U.S. or to another third country?

➔ If your data may be transferred to the U.S. and neither supplementary measures can be provided to ensure that U.S. law does not impinge on the essentially equivalent level of protection as afforded in the EEA provided by the transfer tools, nor derogations under Article 49 GDPR apply, the only solution is to negotiate an amendment or supplementary clause to your contract to forbid transfers to the U.S. Data should not only be stored but also administered elsewhere than in the U.S.

➔ If your data may be transferred to another third country, you should also verify the legislation of that third country to check if it is compliant with the requirements of the Court, and with the level of protection of personal data expected. If no suitable ground for transfers to a third country can be found, personal data should not be transferred outside the EEA territory and all processing activities should take place in the EEA.

For the European Data Protection Board

The Chair

Andrea Jelinek